

WRITE-UP KUALIFIKASI FOSTIFEST CTF 2022

TIM "SOP KAKI KUDA"

KETUA TIM

MUHAMMAD WAHYU SYAFI'UDDIN (encrypt0r)

Category : Bonus

1. Sanity Check



Challenge 21 Solves

Sanity Check

50

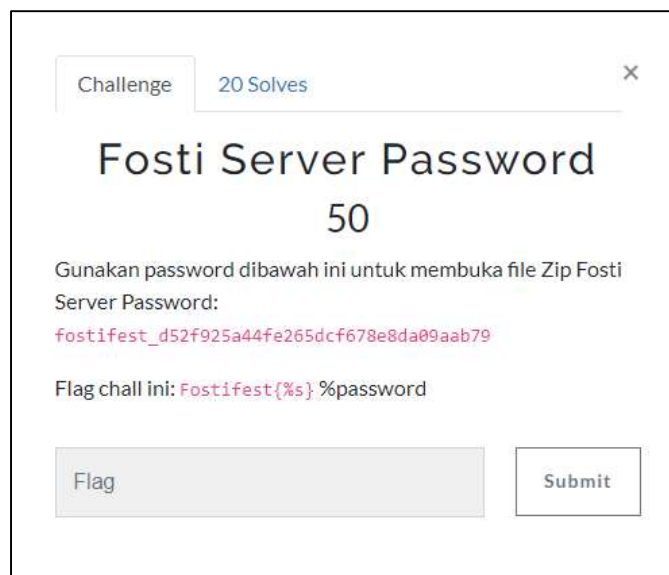
Flag: `Fostifest{Anjazzz_Kelazzzzzzzzz}`

Flag Submit

Hadiah dari kakak Probset :3
Tinggal input aja lah gan. Masa gatau.

`Fostifest{Anjazzz_Kelazzzzzzzzz}`

2. Fosti Server Password



Challenge 20 Solves

Fosti Server Password

50

Gunakan password dibawah ini untuk membuka file Zip Fosti Server Password:

`fostifest_d52f925a44fe265dcf678e8da09aab79`

Flag chall ini: `Fostifest{%s} %password`

Flag Submit

Diatas sudah diberi petunjuk dengan Format Specifiers. Tentu saja, karena %s adalah %password, maka Flag adalah Password ZIP itu sendiri.

`Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}`

3. Feedback

Challenge

0 Solves

×

Feedback

50

Link: <https://forms.gle/f7umuTZr4Ue1EnuDA>

Flag

Submit

Untuk soal Feedback ini, tinggal isi aja feedback di google form terkait, dan akan diberikan Flag setelah submit Form.

Fostifest{__anjazz_kelazzz__}

Category : Forensic

1. The Attacker

Challenge

11 Solves

×

The Attacker

50

Server Fosti yang memiliki beberapa service yang berjalan di dalamnya telah dimasuki oleh hekerz pada sekitar tanggal 20-25 september, diduga kuat hekerz tersebut telah menanamkan banyak backdoor di dalam server. Tugas kalian adalah menyelidiki dan menginvestigasi pada server Fosti agar semua jejak hekerz tersebut terlacak

Pada challenge ini carilah IP dari si Attacker alias Hekerz
Format Flag: `Fostifest{IP-Attacker}`

View Hint

View Hint

1/5 attempts

Flag

Submit

Diberikan sebuah file OVA didalam zip, dan gw mengimport ova tersebut menjadi sebuah VM. Akan tetapi untuk login ke VM terdapat password dari user Ubuntu.

Step yang gw lakukan:

- Boot ke Recovery
- Reset password dengan perintah `passwd ubuntu`
- Masuk ke VM
- Langsung saja gw masuk ke dir `/var/log/`
- Dan setelah gw cek `/var/log/apache2/access.log` tidak terdapat hal menarik, dan ternyata di `/var/log/apache2/access.log.1` ada GET Request dengan perintah yang tidak asing, yaitu perintah buat BackConnect
- Baca perintah tersebut dan terdapat IP address beserta Port
- IP address = 192.168.56.1

Fostifest{192.168.56.1}

2. Initial Access Backdoor

Challenge 9 Solves

Initial Access Backdoor

50

Full path backdoor for initial access in system Flag:
`Fostifest{%s}` Example: `Fostifest{/path/path/path/file}`

View Hint

View Hint

View Hint

2/10 attempts

Flag Submit

Dengan VM yang sama, dan karena sebelumnya sudah melihat access.log maka challenge ini bisa dikatakan ez.

Step yang gw lakukan:

- Melihat adanya GET request ke sebuah file php yang gw duga sebuah minishell
- File di request tersebut adalah `"storage/competition/hacker-CTF-19092022095831.php"`
- Karena diminta Path asli di VM, maka tinggal cari di `/var/www/*`, karena kurang teliti (ngePur -3Jam bg), attempts gw berkurang :((
- Tinggal cari di `/var/www/html/`, dan gw menemukan 2 dir yang memiliki dir storage seperti di Request
- Lagi - lagi kurang teliti, karena gw menginput DIR dari `/var/www/html/storage`, dimana itu gk mungkin di Serve sama aplikasi :((
- Dan akhirnya setelah masuk ke dir public (`/var/www/html/public/storage/competition/hacker-CTF-19092022095831.php`)
Flagnya bner :v

`Fostifest{storage/competition/hacker-CTF-19092022095831.php}`

3. Interactive Shell

Challenge

7 Solves

×

Interactive Shell

247

IP and Port attacker to get interactive shell Format Flag:

`Fostifest{IP:Port}`

Example: `Fostifest{x.x.x.x:xxxx}`

1/5 attempts

Flag

Submit

Masih pada request yang sama (`/var/log/apache2/access.log.1`). pada request tersebut Shell PHP mengeksekusi sebuah command Python dimana setelah konek ke IP:PORT, akan melakukan sebuah `process_call` ke `/bin/sh` dengan flag `-i` dimana, `-i` adalah flag untuk Interactive. Langsung saja tanpa fafifu, input IP dan Port yang gw temukan sebelumnya, yaitu `192.168.56.1:8069`

`Fostifest{192.168.56.1:8069}`

4. The Root

Challenge

1 Solves

×

The Root

472

Woopzzz! Looks like hackerz has a backdoor that is used to call the root user, look for full path of that file Format Flag:

`Fostifest{/path/path/path/file}`

1/5 attempts

Flag

Submit

Karena kondisi yang memacu adrenalin, dengan diBekukan scoreboard, dan kondisi masih Rank 12. Gw langsung ada sedikit ide untuk solve dengan cara Red Team.

Step yang gw lakukan:

- Seperti local enum biasa, gw melakukan pencarian ke SUID Binaries
- Dengan perintah `find / -perm -u=s -type f 2>/dev/null | grep bin` Gw dapat dengan mudah melihat SUID binaries
- Dan akhirnya menemukan binary yang blm pernah gw lihat, yaitu bazh (`/usr/bin/bazh`)
- Langsung saja gw coba eksekusi `bazh`, et voila... User menjadi ROOT

`Fostifest{/usr/bin/bazh}`

5. Re-root Connect

Challenge

3 Solves

×

Re-root connect

437

Looks like hackerz keeps one more backdoor to get root access, looks like he can connect to the machine every minute! Find the full path of this backdoor and the destination IP Port used by the attacker Format Flag:
`Fostifest{/full/path/file:IP:Port}`

1/5 attempts

Flag

Submit

Langsung saja karena waktu yang mepet (-10 menit) dari berakhirnya event. Gw lanjutkan menggunakan metode Red Teaming, Step yang gw lakukan:

- Karena disitu tertulis "every minute" langsung aja gw kepikiran CRON
- Awalnya sedikit lupa dimana letak cron yang mengatur Job per menit. Dan hasilnya muter - muter nyari di `cron.d`, `cron.daily`, `cron.weekly`, `cron.hourly`
- Dan setelah muter-muter seperti helikopter, akhirnya gw liat di `/etc/` kalo disitu ada file `CRONTAB` :((((((
- Tinggal baca `crontab`, dan ... CTF berakhir :v
- Enggk dong, gww masih sempet submit :V

`Fostifest{/etc/crontab:192.168.56.1:42069}`